



National Security Agency/  
Central Security Service



# CYBERSECURITY SOLUTIONS

## COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSfC) SYMMETRIC KEY MANAGEMENT REQUIREMENTS ANNEX V2.0

Version 2.0  
January 2021



# Symmetric Key Management Requirements Annex



## CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Additional Key and Certificate Management Requirements Annex	1.0	21 May 2019	<ul style="list-style-type: none"><li>Initial release of the <i>CSfC Additional Key and Certificate Management Requirements Annex</i>.</li></ul>
CSfC Symmetric Key Management Requirements Annex	2.0	31 January 2021	<ul style="list-style-type: none"><li>Changed document name from <i>CSfC Additional Key and Certificate Management Requirements Annex</i> to <i>CSfC Symmetric Key Management Requirements Annex</i>.</li><li>Updated to add IPsec with RFC 8784-compliant implementations of IKE v2 as an approved protocol for use with Pre-shared Keys (PSKs) in CSfC solutions and removed the use of IKEv1.</li><li>Incorporated MSC CP MACsec Symmetric Key Management requirements from the <i>CSfC Key Management Requirements Annex</i>.</li><li>Replaced Capability Package (CP) requirements mapping column with Threshold / Objective column.</li><li>Updated Appendix B: References.</li><li>Minor administrative changes were made in formatting.</li></ul>



# Symmetric Key Management Requirements Annex



## Table of Contents

1	Introduction and Purpose .....	5
2	Pre-Shared Keys (PSKs) .....	5
2.1	Overview of Pre-Shared Keys (PSKs) in CSfC Solutions .....	5
2.2	Overview of Symmetric Key Generation Solutions .....	7
2.3	PSK Implementation Requirements .....	9
2.3.1	PSK Generation, Distribution, and Installation .....	9
2.3.2	PSK Usage .....	15
2.3.3	PSK Update .....	16
2.3.4	PSK Compromise Recovery .....	19
2.3.5	KGS Connectivity Guidance .....	23
2.3.6	KGS Audit Guidance .....	24
2.3.7	PSK Testing Guidance .....	25
	APPENDIX A. – Acronyms .....	26
	APPENDIX B. - Reference .....	27
	APPENDIX C. – Sample Structure For A Key and Certificate Management Plan (KCMP) .....	29

## Table of Figures

Figure 1: PSK Management Services .....	7
Figure 2: CSfC Security Device Management for PSKs .....	8
Figure 3: PSK Generation, Distribution and Installation into a CSfC Security Device .....	10
Figure 4: PSK Update for a CSfC Security Device .....	18
Figure 5: PSK Compromise Recovery for CSfC Security Devices .....	20
Figure 6: Connectivity Guidance for Locally Operated Key Generation Solutions .....	23

## List of Tables

Table 1: Applicability of PSKs to CSfC Capability Packages .....	6
Table 2: PSK Generation, Distribution and Installation Requirements for CSfC Solutions .....	10
Table 3: PSK Usage Requirements for CSfC Solutions .....	15



# Symmetric Key Management Requirements Annex



Table 4: PSK Update Requirements for CSfC Solutions.....	18
Table 5: PSK Compromise Recovery Requirements for CSfC Solutions .....	20
Table 6: KGS Connectivity Requirements for CSfC Solutions.....	23
Table 7: Additional KGS Audit Requirements for CSfC Solutions.....	24
Table 8: PSK Testing Requirements for CSfC Solutions.....	25



# Symmetric Key Management Requirements Annex



## 1 INTRODUCTION AND PURPOSE

This document serves as a design addendum for Commercial Solutions for Classified (CSfC) and specifically defines additional requirements for implementing symmetric key management capabilities defined in CSfC Capability Packages (CPs) to ensure symmetric keys are implemented correctly and securely within CSfC solutions.

## 2 PRE-SHARED KEYS (PSKS)

This section provides implementation requirements for the use of PSKs within CSfC solutions.

### 2.1 Overview of Pre-Shared Keys (PSKs) in CSfC Solutions

Symmetric Pre-Shared Keys (PSKs) may be used instead of X.509 v3 authentication certificates to provide quantum resistant cryptographic protection of classified information within CSfC solutions. For CSfC customers who have a requirement to protect long-life<sup>1</sup> classified intelligence information, one of the two CSfC solution tunnels uses PSKs to provide the required quantum resistant cryptographic protection for that information. The second tunnel uses X.509 v3 authentication device certificates per the requirements of the applicable CP. PSKs are only required for one security tunnel to minimize the risks associated with PSK management, and specifically the risk of disclosing the PSKs in an unauthorized manner. Additionally, PSKs are used for Media Access Control Security (MACsec) devices in solutions that comply with the Multi-Site Connectivity (MSC) CP. PSKs for MACsec devices are referred to as Connectivity Association Keys (CAKs) in the MSC CP. Every CAK has a unique Connectivity Association Key Name (CKN) to distinguish it from other CAKs that may be loaded in the MACsec Device.

When PSKs are required in a CSfC solution, they are used for the inner tunnel when possible to: (a) apply quantum resistant cryptographic protection directly to plaintext classified information, and (b) mitigate risks associated with the compromise of outer tunnel PSKs that permit an adversary to perform an undetected Man-in-the-Middle (MitM) attack on the outer gateway of a CSfC solution that further allows the adversary to attempt attacks on the inner tunnel. In some cases, PSKs cannot be used for the inner tunnel if the inner tunnel protocol is not approved for use with PSKs (e.g., Mobile Access CP where the inner tunnel uses Transport Layer Security [TLS] version 1.2). Internet Protocol Security (IPsec) with Internet Engineering Task Force (IETF) Request for Comments (RFC) 8784-compliant implementations of Internet Key Exchange (IKE) v2 and MACsec are approved protocols that can use PSKs in CSfC solutions. Other protocols may be approved in the future by the CSfC program office<sup>2</sup>. Table 1, summarizes where PSKs are used in the various CSfC solutions. More detailed implementation requirements for PSKs in these CSfC solutions is provided in sections 2.3.1 through 2.3.7

---

<sup>1</sup> Long-life is defined as 20 years or longer.

<sup>2</sup> The CSfC program office plans to approve TLS 1.3 for use with PSKs in the future.



# Symmetric Key Management Requirements Annex



**Table 1: Applicability of PSKs to CSfC Capability Packages**

Capability Package	PSK Implementation: Inner Tunnel vs. Outer Tunnel
Mobile Access (MA)	If the inner tunnel uses IPsec AND there is only one Red Network enclave in the solution, then PSKs are to be implemented on the inner tunnel with IPsec RFC 8784-compliant IKE v2. Else, PSKs are to be implemented on the outer tunnel with IPsec RFC 8784-compliant IKE v2 (i.e., when the inner tunnel is either TLS or SRTP, or when there are multiple Red Network enclaves in the solution).
Campus Wireless Local Area Network (WLAN)	The inner tunnel always uses IPsec. Therefore, PSKs are to be implemented on the inner tunnel with IPsec RFC 8784-compliant IKE v2.
Multi-Site Connectivity (MSC)  There are four configurations supported by the MSC CP: 1. Outer VPN Device and Inner VPN Device 2. Outer VPN Device and Inner MACsec Device 3. Outer MACsec Device and Inner VPN Device 4. Outer MACsec Device and Inner MACsec Device	For each configuration, PSKs are implemented as follows: 1. PSKs are implemented on the inner tunnel VPN Device with IPsec RFC 8784-compliant IKE v2. 2. PSKs are used per the MSC CP for the inner tunnel MACsec Device; therefore, PSKs are not used for the outer tunnel VPN Device. 3. PSKs are used per the MSC CP for the outer tunnel MACsec Device; therefore, PSKs are not used for the inner tunnel VPN Device. 4. PSKs are used per the MSC CP for both MACsec Devices.

CSfC customers need to be aware of the risks involved in using PSKs. First, PSKs need to be of adequate strength for them to be used to access and protect classified information. Second, PSKs need to be securely generated, distributed, installed, and managed to mitigate the risk of unauthorized disclosure of the PSKs (e.g., insider threat). A compromised PSK permits a MitM attack, and affects at least two CSfC solution components. Upon detection of a compromised PSK, CSfC solution components that use that PSK need to be updated with a new PSK. This is different from the X.509 certificate-based solutions in that revocation of any given certificate only affects the device associated with that certificate. Therefore, PSK management, which includes the generation, distribution, installation, update, destruction, and accounting of symmetric PSKs, is a critical function for CSfC solutions that use PSKs. PSK management can be provided by enterprise services or via locally operated solutions. The PSK implementation requirements defined in this document applies to both enterprise and locally operated symmetric key generation and management solutions used to support PSK management within CSfC solutions.



# Symmetric Key Management Requirements Annex



## 2.2 Overview of Symmetric Key Generation Solutions

A National Security Agency (NSA)-approved<sup>3</sup> Key Generation Solution (KGS) is used to generate and manage PSKs for a CSfC solution as shown in Figure 1.

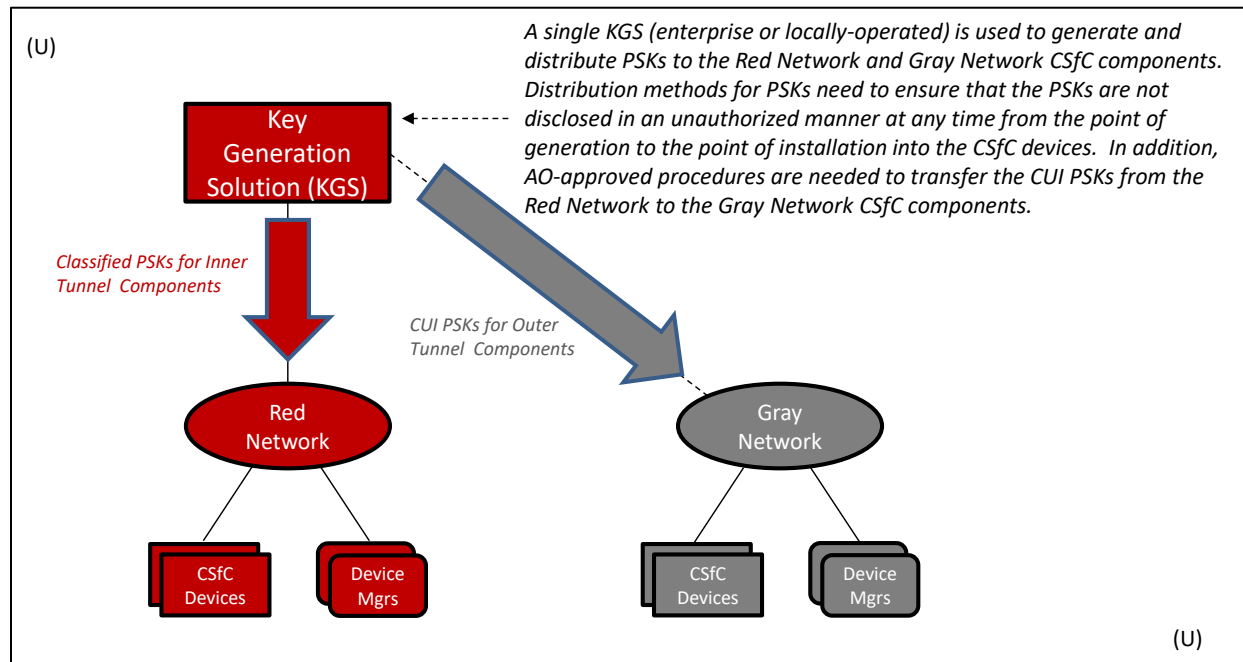


Figure 1: PSK Management Services

The KGS generates and distributes PSKs (per the guidance in Table 1) to CSfC devices operating in the Red and Gray Networks, where the KGS operates in the Red Network. Device Managers (DMs) are used to ensure distribution and installation of PSKs onto CSfC devices is performed securely and in a trustworthy manner. PSKs used for inner tunnel components operating on the Red/Gray Network boundary are classified to the level of the Red Network. PSKs used for outer tunnel components operating on the Gray/Black network boundary are Controlled Unclassified Information (CUI), and are distributed in accordance with approved procedures<sup>4</sup> to move the PSKs from the Red Network to the Gray Network.

The role of the DM in the CSfC solution is further described in Figure 2. The DM requests a PSK from the KGS, and the KGS verifies that the request came from an authorized DM. The KGS generates the PSK and securely distributes the PSK to the DM. Secure distribution can be achieved via technical means

<sup>3</sup> NSA-approved means: (a) a component from the CSfC Approved Products List, (b) a component approved for the CSfC solution by the Deputy National Manager for National Security Systems; or (c) an already approved enterprise service.

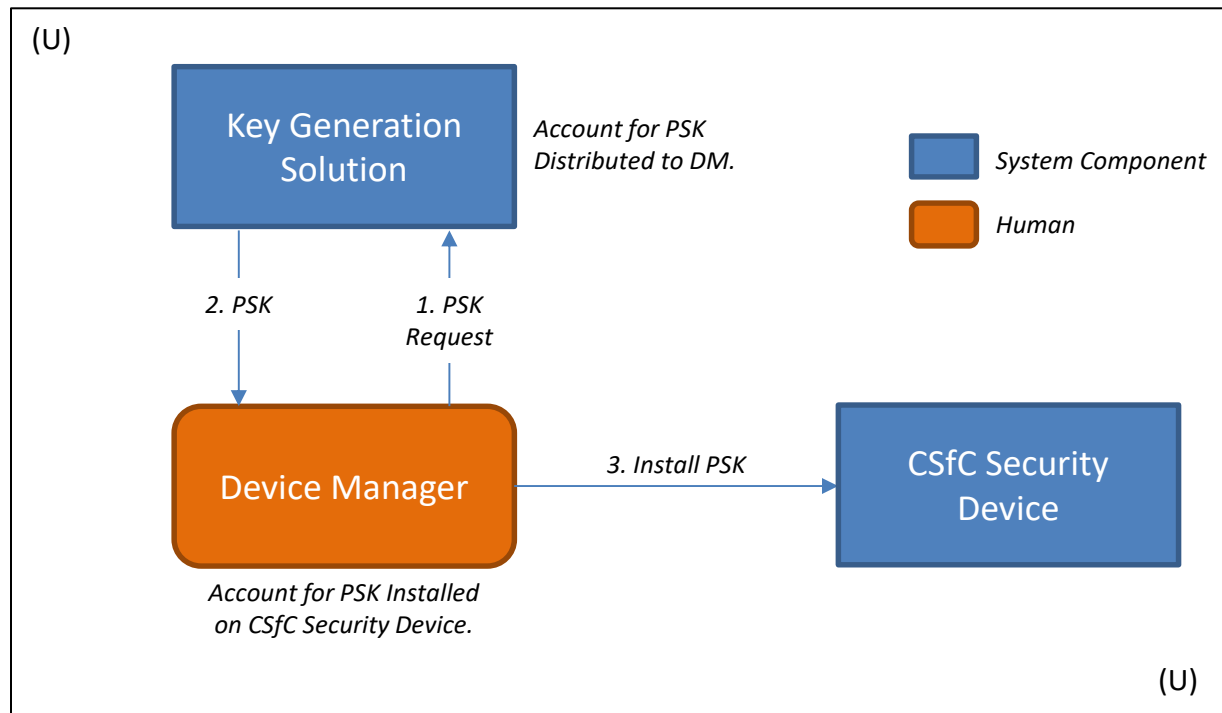
<sup>4</sup> The local Authorizing Official (AO) approves the procedures.



# Symmetric Key Management Requirements Annex



(e.g., encryption) or procedural controls. The DM then installs the PSK into the security device, and destroys/deletes any remaining copies of the PSK.<sup>5</sup> Installation is likely performed with the PSK in red form given current capabilities of CSfC solution components.<sup>6</sup> Future capabilities may allow an encrypted form of the PSK to be installed, thereby limiting exposure of the PSK.



**Figure 2: CSfC Security Device Management for PSKs**

The KGS and DM also account for the PSK to ensure its location (i.e., the CSfC component containing the PSK) is known at all times. In case of compromise, the KGS and DM need to be able to determine where all instances of a given PSK exist (i.e., all CSfC components containing the compromised PSK) and update that PSK in accordance with compromise reporting and recovery procedures.

Preferably, the DM and the KGS are network-connected and operate in the same network domain and at the same classification level. In some cases, the DM and KGS operate in different network domains, and potentially at different classification levels. In the latter case, procedures need to be developed and

<sup>5</sup> Removable media, electronic files and memory containing PSKs must be destroyed / deleted using AO-approved procedures and in accordance with CNSSI 4004. This requirement does not apply to storing approved backup copies of the PSK.

<sup>6</sup> The DM may use, if approved by the local AO, a management workstation to establish a secure and authenticated connection to the CSfC Device to install the PSK (e.g., SSH). However, SSH and other similar protocols are not quantum-resistant key distribution protocols, and the risk for installing the PSK in this manner must be taken into consideration.



# Symmetric Key Management Requirements Annex



approved by the local Authorizing Official (AO) to ensure the secure and accurate transfer of information between the DM and KGS. (See Section 2.3.5 for connectivity examples.)

Finally, an approved Key and Certificate Management Plan (KCMP) is required that fully describes the life-cycle management of PSKs that are generated by the KGS. The KCMP addresses requirements and controls defined in *CNSSI 4005: Safeguarding COMSEC Facilities and Materials*. For classified PSKs, the requirements and controls defined in CNSSI 4005 are to be strictly adhered to.<sup>7</sup> For CUI PSKs, CNSSI 4005 is to be used as guidance to define requirements that ensure the secure distribution of PSKs onto CSfC solution components, and the mapping of PSKs to those components for accountability and compromise reporting purposes. Reference *Appendix C. – Sample Structure for a Key and Certificate Management Plan (KCMP)* for additional guidance.

## 2.3 PSK Implementation Requirements

This section defines additional implementation requirements for the use of PSKs in CSfC solutions. Areas addressed include PSK generation, distribution and installation; PSK usage; PSK update (rekey)<sup>8</sup>; PSK compromise recovery; KGS connectivity; KGS audit; and PSK testing.

### 2.3.1 PSK Generation, Distribution, and Installation

The generation, distribution and installation of PSKs for CSfC solutions is shown in Figure 3. An NSA-approved KGS is used to centrally generate and manage PSKs for CSfC security devices, where two CSfC security devices are required to receive and store the same PSK. The two security devices are used to establish either the outer tunnel or inner tunnel for the CSfC solution. One of the DMs within the CSfC solution initiates a request to the KGS for a PSK. The KGS verifies the request came from an authorized DM and generates a PSK in accordance with the approved KCMP. The KGS assigns a unique identifier<sup>9</sup> to the PSK for accounting purposes and distributes the PSK to the DMs that are responsible for installing the PSK onto the CSfC security devices. Preferably, the PSK is encrypted for distribution to each DM either using an approved password-based encryption algorithm, a pre-placed symmetric key that is shared between the KGS and each DM, or using a quantum-resistant key distribution protocol. The pre-placed PSK Encryption Key (PEK) is generated by the KGS and distributed out of band to the DM. A separate PEK should be used for each DM.

---

<sup>7</sup> Specific attention should be provided to Section VII: Physical Security of COMSEC Material; Section VIII: Electronic Key Management System; Section IX: Key Management Infrastructure; Section X: COMSEC Account / KOA Managers; Section XI: Accounting, Inventory and Audits; Section XII: Issuing and Using COMSEC Material; Section XIII: Encrypted COMSEC Material; and Section XIV: Transportation of COMSEC Material.

<sup>8</sup> PSK update means the same thing as PSK rekey; that is, a new PSK is provided during the update process. The term “update” is used to better align with commercial terminology.

<sup>9</sup> The unique identifier may be a technical computation based on the PSK (e.g., hash of the PSK) or it may be a manually generated identifier.



# Symmetric Key Management Requirements Annex



Each DM acknowledges receipt of the PSK back to the KGS, and the KGS keeps an accounting record of the PSKs delivered to each DM based on the unique identifiers assigned to the PSKs. Each DM is then responsible for installing the PSK on the CSfC security device managed by the DM. PSK installation is typically performed in plaintext form, as that is the common format supported by the CSfC security device. Future capabilities may allow PSK installation to be performed using encryption. After PSK installation is complete, the DMs keep an accounting record to know which PSKs are installed on each CSfC security device using the identifier assigned by the KGS.

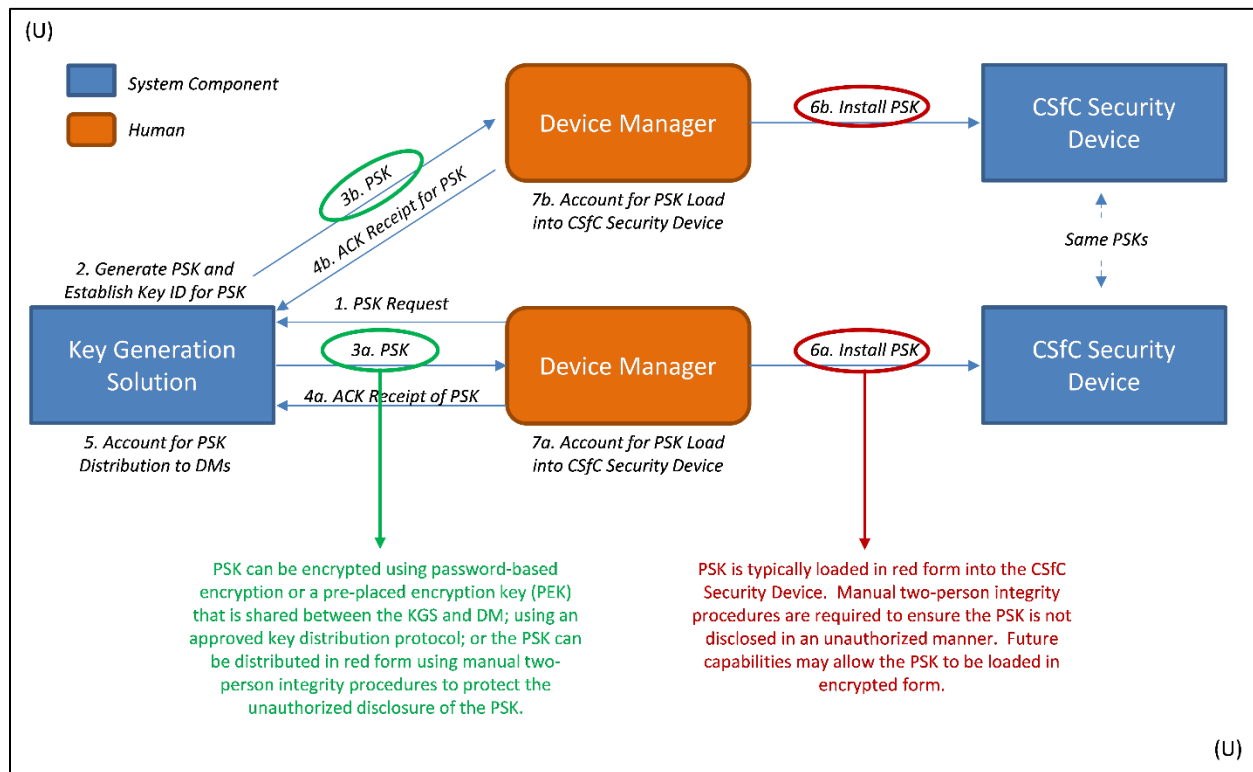


Figure 3: PSK Generation, Distribution and Installation into a CSfC Security Device Table 2 summarizes general requirement statements for PSK generation, distribution and installation. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully, and securely, implementing the techniques for generation, distribution and installation of PSKs within the CSfC solution.

Table 2: PSK Generation, Distribution and Installation Requirements for CSfC Solutions



# Symmetric Key Management Requirements Annex



Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-1	Generation of PSKs must be performed by an NSA-approved Key Generation Solution (KGS). NSA-approved means: (a) a component from the CSfC Approved Products List, (b) a component approved for the CSfC solution by the Deputy National Manager for National Security Systems, or (c) an already approved enterprise service.	Contact the CSfC PMO to identify an NSA-approved KGS that can be used within a CSfC solution.	T=O
PSK-2	Centralized generation, distribution, installation and management of PSKs must be performed by a dedicated KGS.	Deploy a single KGS within the Red Network of the CSfC solution and in accordance with operational deployment instructions provided by the CSfC PMO or the enterprise KGS. In addition, a KCMP needs to be developed that fully describes the life-cycle management of PSKs that are generated by the KGS. See <i>Appendix C. – Sample Structure for a Key and Certificate Management Plan (KCMP)</i> for a sample structure of a KCMP.	T=O
PSK-3	PSKs must always be 256 bits.	Configure the KGS to generate 256 bit PSKs.	T=O
PSK-4	PSKs must not be exposed in plaintext form once they have been packaged by the KGS for distribution and until they are ready to be installed onto CSfC components. Installation of PSKs is typically performed via file transfer or text input.  Note: PSKs may be in plaintext form when generated at the KGS. This guidance applies to the distribution and installation of PSKs.	Technical and procedural controls must be used to ensure PSKs are not exposed in plaintext form during the distribution process and until just prior to installation into a CSfC security device. Technical controls include encryption of the PSKs (e.g., encryption of PSKs on removable media, encryption of PSKs in electronic message exchange). Procedural controls use cleared and trusted personnel and AO-approved procedures. Technical and procedural controls may also be combined. For example, a PSK is encrypted at the KGS and placed on	T=O



# Symmetric Key Management Requirements Annex



Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective
		removable media (e.g., CD, USB Drive). The password to decrypt the PSK is provided to one cleared and trusted person, and the removable media containing the encrypted PSK is provided to a second cleared and trusted person. The two authorized individuals distribute the PSK and password to the CSfC device, where one individual inserts the removable media into the CSfC device and the other individual enters the password to decrypt the PSK.	
PSK-5	PSKs must be protected from unauthorized disclosure when they are distributed outside of a controlled boundary or over unprotected communications channels.	If PSKs are distributed electronically over an unprotected network, they must be encrypted using quantum resistant techniques. If PSKs are distributed manually and outside of a controlled boundary, they must be distributed by cleared and trusted personnel using AO-approved and CNSSI 4005 defined Two-Person Integrity (TPI) <sup>10</sup> procedures to ensure that no one person has sole access to the plaintext PSK.	T=O
PSK-6	Encryption of PSKs must be performed using a password-based encryption algorithm; pre-placed symmetric PEKs; or using a quantum resistant key distribution protocol.	NSA-approved cryptographic solutions must be used for password-based encryption algorithms, PEKs and quantum resistant key distribution protocols.	T=O
PSK-7	PEKs must always be 256 bits.	Configure the KGS to generate 256 bit PEKs.	T=O
PSK-8	Passwords used with a password-based encryption algorithm must be randomly generated using an	<i>No additional requirements.</i>	T=O

<sup>10</sup> Two-Person Integrity (TPI) procedures as defined in CNSSI 4005 must be applied throughout the entire life-cycle management of PSKs and PSK Encryption Keys (PEKs), starting with generation, and through distribution, installation, update and destruction. No one person shall have sole access to the plaintext PSK or PEK at any time during the life-cycle management of PSKs and PEKs.



# Symmetric Key Management Requirements Annex



Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective
	NSA-approved password generation tool.		
PSK-9	The password length guidance provided in the <i>CSfC Data-At-Rest CP</i> must be followed to determine the required minimum password length.	Follow the password strength guidance provided in the CSfC Data-At-Rest Capability Package to determine the minimum password length.	T=O
PSK-10	Passwords must be different each time a PSK is encrypted using a password-based encryption algorithm.	A new and different password must be used each time a PSK is encrypted using a password-based encryption algorithm. Passwords must not be reused.	T=O
PSK-11	PSKs issued to Outer Encryption Components are classified as determined by the AO and compliant with CNSSI 4005.	<i>No additional requirements.</i>	T=O
PSK-12	PSKs issued to Inner Encryption Components are classified to the level of the Red network.	<i>No additional requirements.</i>	T=O
PSK-13	The classification of pre-placed PEKs and passwords is the same as the classification of the PSKs that they are protecting.	<i>No additional requirements.</i>	T=O
PSK-14	Manual distribution procedures and methods may be used for PSKs when encryption of PSKs is not feasible.	If PSKs are distributed manually and outside of a controlled boundary, they must be distributed by cleared and trusted personnel using AO-approved and CNSSI 4005 defined TPI procedures to ensure that no one person has sole access to the plaintext PSK.	T=O
PSK-15	PSKs and PEKs must be identified using unique key identifiers.	Technical or procedural methods are to be used to uniquely identify each PSK generated by the KGS. A technical method is to hash the PSK/PEK and use the hash value as the key identifier. The PSK/PEK identifiers must be unique within a given CSfC solution.	T=O
PSK-16	PSKs and PEKs must be accounted for throughout their life cycles.	Technical or procedural methods are to be used to account for each	T=O



# Symmetric Key Management Requirements Annex



Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective
	Specifically, the KGS needs to account for PSKs and PEKs distributed to DMs, and DMs need to account for PSKs and PEKs installed on CSfC security devices.	PSK generated by the KGS during the life-cycle of the PSK, where life-cycle includes: 1) PSK generation, 2) PSK receipt by the DM to the KGS, 3) PSK installation into the CSfC device, 4) PSK update by the DM, which includes generation of a new PSK by the KGS, receipt of the new PSK by the DM to the KGS, and installation of the new PSK into the CSfC device, and; 5) PSK compromise notification and recovery, which includes identifying the PSK as compromised, removing copies of the compromised PSK from the CSfC solution, and updating the required CSfC devices with a new PSK.	
PSK-17	Accounting procedures for classified PSKs and PEKs must comply with CNSSI 4005 controls and requirements.	CNSSI 4005 accounting procedures for classified PSKs and PEKs may be tailored as needed for the CSfC solution, but must be approved by the AO.	T=O
PSK-18	Accounting procedures for PSKs and PEKs designated as CUI should leverage CNSSI 4005 controls and requirements. At a minimum, accounting procedures will include: (a) mapping of PSK and PEK unique key identifiers to CSfC components; and (b) individual receipt confirmation for PSKs and PEKs during the distribution process.	CNSSI 4005 accounting procedures for CUI PSKs and PEKs may be tailored as needed for the CSfC solution, but must be approved by the AO.	T=O
PSK-19	All life-cycle management for PSKs, passwords, and PEKs, from generation through destruction, must be performed in accordance with the approved KCMP.	See APPENDIX C. – Sample Structure For A Key and Certificate Management Plan (KCMP) for a sample structure of a KCMP or use the KCMP provided by the enterprise KGS.	T=O



# Symmetric Key Management Requirements Annex



Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-20	Any backups of PSKs and PEKs must be performed in accordance with CNSSI 4005 Section VII.D [Storage of COMSEC Material], Section XI [Accounting, Inventory and Audits], and Section XIII [Encrypted COMSEC Material], or other NSA-approved procedures.	CNSSI 4005 accounting procedures for classified PSKs and PEKs may be tailored as needed for the CSfC solution, but must be approved by the AO.	T=O

## 2.3.2 PSK Usage

PSKs are used by CSfC security devices to perform mutual authentication of the devices that establish the CSfC inner or outer security tunnels. Once the PSK is installed into a CSfC security device, the PSK is assumed valid until it requires updating (see

Table 4 and Table 5). Therefore, no additional validation needs to be performed by the CSfC security device prior to using the PSK. This is different from the X.509 certificate-based CSfC solutions that require the certificates to be validated before they are used for authenticating the inner and outer tunnels.

Since there is no additional validation performed on the PSKs, it is critical that the PSKs (and PEKs, if they are used) be stored securely within the CSfC security device to prevent unauthorized disclosure of the PSK/PEK. In addition, any export of the PSK/PEK needs to ensure that the plaintext version of the PSK/PEK is not disclosed in an unauthorized manner.

Table 3 summarizes general requirement statements for the usage of PSKs. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully, and securely, implementing the techniques for the usage of PSKs within the CSfC solution.

**Table 3: PSK Usage Requirements for CSfC Solutions**

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-21	PSKs must only be used with CSfC protocols that are approved for use with PSKs.	See Table 1.	T=O
PSK-22	PSKs must be stored within a CSfC component in encrypted form.	CSfC security devices using PSKs are to be chosen from an approved list of devices defined by the CSfC	T=O



# Symmetric Key Management Requirements Annex



Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
		Program Office. Approved devices incorporate acceptable protection of PSKs within those devices by storing the PSKs in encrypted form.	
PSK-23	PSKs and PEKs exported from a CSfC component must be protected from unauthorized disclosure. Encryption of exported PSKs and PEKs is recommended; however, manual procedure protection methods may be used when encryption of exported PSKs and PEKs is not technically feasible.	Technical and procedural controls must be used to securely export PSKs and PEKs from a CSfC device. Technical controls use quantum resistant techniques to encrypt the PSKs and PEKs. Manual controls use trusted and cleared personnel operating under TPI procedures, along with AO-approved storage containers to securely store the PSKs and PEKs.	T=O
PSK-24	A compromised PSK/PEK must never be used in a CSfC solution.	<i>No additional requirements.</i>	T=O
PSK-25	Each PSK and PEK must be uniquely identified to ensure a compromised PSK/PEK is never used in a CSfC solution.	Unique identification of the PSK/PEK may be performed using technical or procedural methods.	T=O
PSK-26	PSKs must not be shared by more than two CSfC security devices.	Group keys must not be used in CSfC solutions.	T=O

## 2.3.3 PSK Update

PSKs require periodic updating<sup>11</sup> to limit the amount of operational exposure for the PSKs. If a PSK existed for a long operational time, and an adversary was able to compromise the PSK without detection, the adversary would be able to use the PSK (i.e., commit a man-in-the-middle attack) until the PSK was updated. Frequent updates of PSKs minimize the window of opportunity an adversary may have in compromising and using the PSK before being detected. Therefore, considerations for periodicity of PSK updates include:

- *The number of CSfC solution components that share the same PSK* – As more components share the same PSK, the more frequent the PSK updates should occur. This document requires that PSKs only be used in pairwise configurations (i.e., only two devices share a given PSK).

<sup>11</sup> In this guidance, PSK update refers to a new key being installed in the CSfC device. Therefore, PSK update is synonymous with PSK rekey.



# Symmetric Key Management Requirements Annex



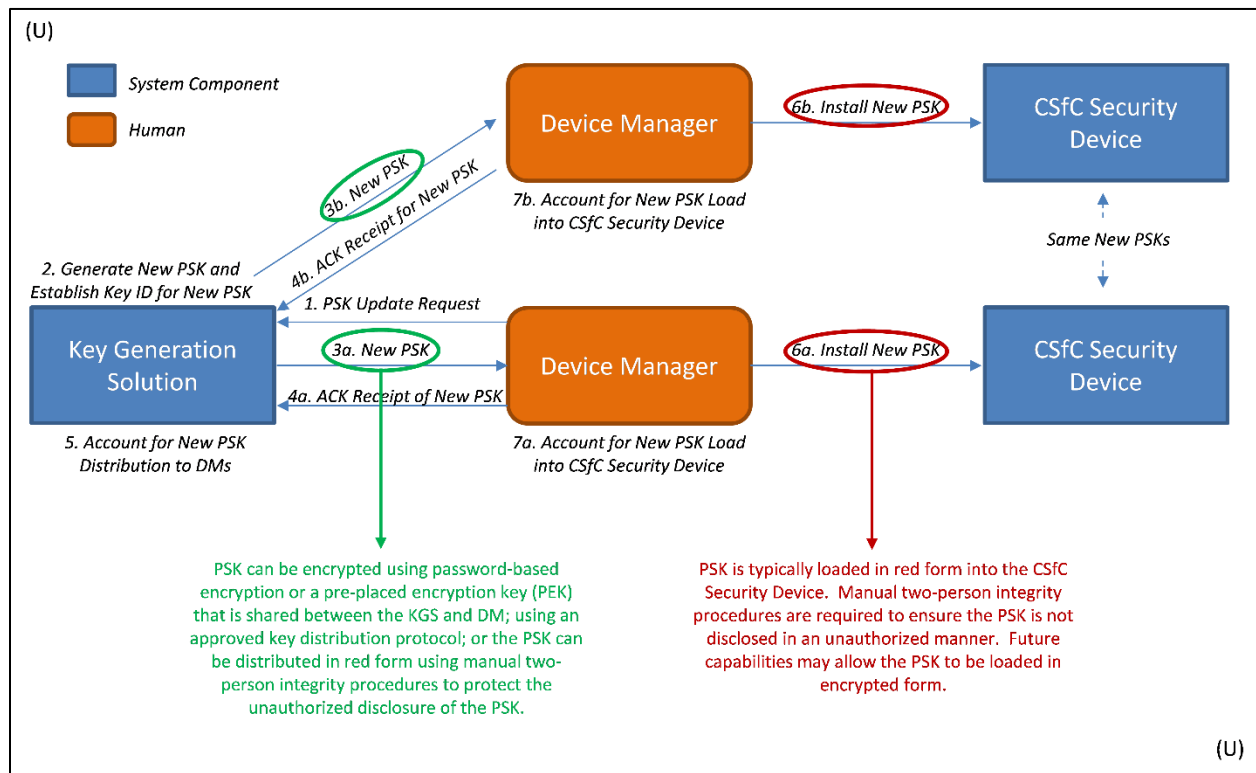
- *Sensitivity of the information being protected by the CSfC solution that uses PSKs* – As the sensitivity level of the information increases, the more frequent the PSK updates should occur.
- *Accessibility or level of difficulty to compromise a CSfC solution component and the PSK* – As the level of accessibility increases (or level of difficulty decreases), the more frequent the PSK updates should occur.

The PSK update process is shown in Figure 4, which is the same as the PSK generation, distribution and installation process shown in Figure 3. One of the DMs within the CSfC solution initiates an update request to the KGS for a new PSK. The KGS verifies the request came from an authorized DM and generates a new PSK in accordance with the approved KCMP. The KGS assigns a unique identifier to the PSK for accounting purposes and distributes the new PSK to the DMs that are responsible for installing the new PSK onto the CSfC security devices. Preferably, the new PSK is encrypted for distribution to each DM using either an approved password-based encryption algorithm, a PEK that is shared between the KGS and each DM, or a quantum resistant key distribution protocol. The PEK can be generated by the KGS and distributed out of band to the DM. A separate PEK should be used for each DM.

Each DM acknowledges receipt of the new PSK back to the KGS, and the KGS keeps an accounting record of the new PSKs delivered to each DM based on the unique identifiers assigned to the PSKs. Each DM is then responsible for installing the new PSK on the CSfC security device managed by the DM. PSK installation is typically performed in plaintext form, as that is the common format supported by the CSfC security device. Future capabilities may allow PSK installation to be performed using encryption. After the new PSK is installed, the DMs keep an accounting record to know which new PSKs are installed on each CSfC security device using the identifier assigned by the KGS.



# Symmetric Key Management Requirements Annex



**Figure 4: PSK Update for a CSfC Security Device**

Table 4 summarizes general requirement statements for the update of PSKs. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully, and securely, implementing techniques for the updating of PSKs within the CSfC solution.

**Table 4: PSK Update Requirements for CSfC Solutions**

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-27	PSKs must be updated every 30 to 180 days, or as required by the KCMP.	<ul style="list-style-type: none"><li>Updating of PSKs follows the same implementation requirements defined in Section 2.3.1 for PSK generation, distribution and installation.</li><li>The KCMP must define the periodicity of PSK updates for the CSfC solution.</li></ul>	T=0



# Symmetric Key Management Requirements Annex



Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-28	PEKs must be updated every 90 days, or as required by the KCMP.	Updating of PEKs follows the same implementation requirements defined in Section 2.3.1 for PSK generation, distribution and installation.	T=0

## 2.3.4 PSK Compromise Recovery

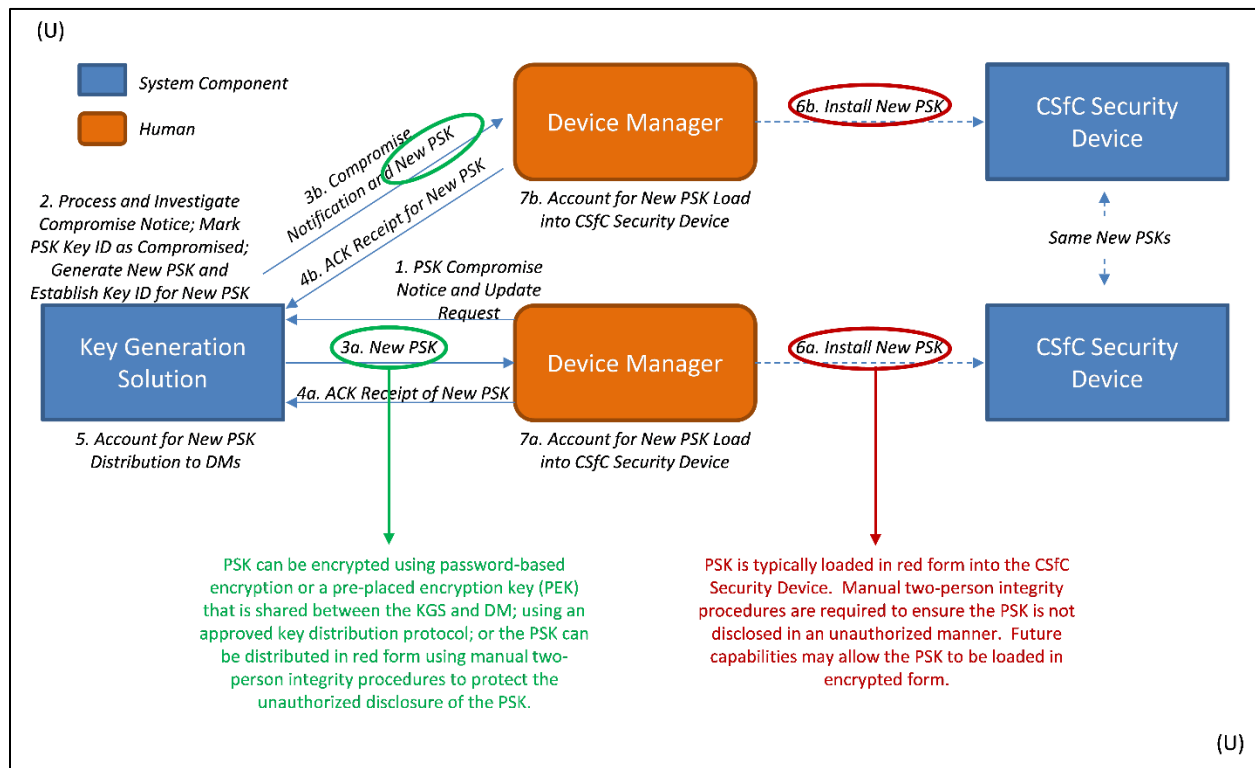
PSK compromise recovery is a critical function within a CSfC solution<sup>12</sup>. Because a PSK is shared between two CSfC security devices, compromise of one device and its PSK ends up compromising the other device that shares the same PSK. Therefore, the CSfC solution must maintain accurate accounting records to know which PSKs are installed on which CSfC security devices. The KGS needs to be able to contact DMs and inform them of a PSK compromise. The DMs then need to determine which CSfC security devices use the compromised PSK, and execute the *PSK Update* process to replace the compromised PSK.

Figure 5 shows the PSK compromise recovery process. The process begins with one of the DMs detecting a PSK compromise, suspending the use of the PSK, and sending a compromise notification to the KGS that a particular PSK has been compromised, along with a PSK update request to obtain a new PSK. Using the unique key identifier assigned to the PSK, the KGS is able to determine the other DM that was provided with the same PSK that was compromised. The KGS generates a new PSK and distributes the new PSK to the DMs that require it. The KGS also informs the remaining DM that the prior PSK was compromised, thereby providing rationale for the distribution of the new PSK. The DMs acknowledge receipt of the new PSK back to the KGS, ensure that the compromised PSK is removed and no longer used, and install the new PSK onto the CSfC security devices.

<sup>12</sup> CNSSI 4003 is the authoritative source for reporting and evaluating COMSEC incidents.



# Symmetric Key Management Requirements Annex



**Figure 5: PSK Compromise Recovery for CSfC Security Devices**

Table 5 summarizes general requirement statements for the compromise recovery of PSKs. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully, and securely, implementing techniques for the compromise recovery of PSKs within the CSfC solution.

**Table 5: PSK Compromise Recovery Requirements for CSfC Solutions**

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-29	Accounting procedures must support PSK and PEK compromise recovery to ensure all copies of compromised PSKs and PEKs are identified and updated (rekeyed).	Technical or procedural methods are to be used to support PSK/PEK compromise notification and recovery, which includes identifying the PSK/PEK as compromised, removing copies of the compromised PSK/PEK from the CSfC solution, and updating the required CSfC devices with a new PSK. CNSSI 4003 and 4005 are to be used to develop the	T=0



# Symmetric Key Management Requirements Annex



Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
		compromise notification and recovery procedures.	
PSK-30	The PSK/PEK compromise recovery process must be documented in the KCMP.	CNSSI 4003 and 4005 are to be used to develop the compromise notification and recovery procedures. See <i>Appendix C. – Sample Structure for a Key and Certificate Management Plan (KCMP)</i> for a sample structure of a KCMP or the KCMP provided by the enterprise KGS.	T=O
PSK-31	PSKs/PEKs must be updated (rekeyed) as soon as practically possible if they are considered compromised.	Updating of PSKs/PEKs follows the same implementation requirements defined in Section 2.3.1 for PSK generation, distribution and installation.	T=O
PSK-32	The DM must determine if a PSK/PEK is considered compromised, and submit a compromise notification to the KGS along with a request to update the PSK/PEK.	The DM submits a compromise notification using a procedure that is agreed upon with the KGS, such that the KGS can trust the authenticity of the compromise notification (e.g., signed email, signed form). CNSSI 4003 and 4005 are to be used to develop the compromise notification and recovery procedures.	T=O
PSK-33	The DM and KGS must follow procedures for PSK/PEK compromise reporting as defined by the applicable KCMP.	CNSSI 4003 and 4005 are to be used to develop the compromise notification and recovery procedures. See <i>Appendix C. – Sample Structure for a Key and Certificate Management Plan (KCMP)</i> for a sample structure of a KCMP or the KCMP provided by the enterprise KGS.	T=O
PSK-34	Compromise recovery procedures must include response to a lost, stolen or compromised End User Device (EUD).	The DM of an EUD is to be notified when the device is lost, stolen or compromised so that the DM can report the PSK associated with the device as compromised. All other devices that share the same PSK are to be considered compromised and	T=O



# Symmetric Key Management Requirements Annex



Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
		the PSKs for all devices need to be updated.	
PSK-35	Compromise recovery procedures must include removal of a compromised infrastructure device (e.g., VPN Gateway) from the network.	<p>If an infrastructure device is determined to be compromised, the DM of the infrastructure device needs to physically disconnect the device from the network when the device is considered compromised, and only reconnect the device to the network after all of the compromised PSKs associated with that device are successfully updated. The DM also needs to identify all other devices that share the PSKs of the compromised infrastructure device so that those devices can have their PSKs updated.</p> <p>If an EUD is compromised, an assessment needs to be made if the infrastructure device is to be removed from the network prior to updating the PSK in the infrastructure device.</p>	T=O
PSK-36	Compromise recovery procedures must address re-establishing a CSfC security device after its PSK is compromised.	Re-establishment of PSKs follows the same implementation requirements defined in Section 2.3.1 for PSK generation, distribution and installation.	T=O
PSK-37	If a compromised device is to be reused, that device must go through the initial PSK issuance process.	Reuse of a compromised CSfC security device follows the same implementation requirements defined in Section 2.3.1 for PSK generation, distribution and installation. This requirement is in addition to the Capability Package requirements for reusing a compromised device.	T=O

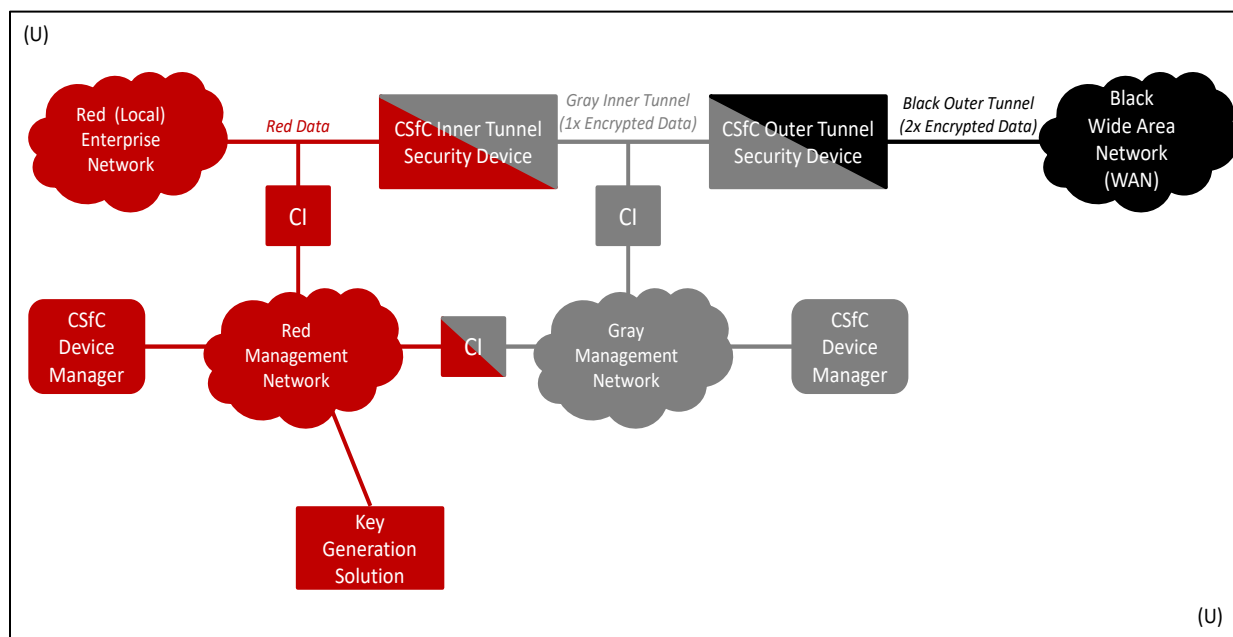


# Symmetric Key Management Requirements Annex



## 2.3.5 KGS Connectivity Guidance

Figure 6 addresses connectivity of a KGS into CSfC solutions. The KGS connects with the local red management network and provides PSK management services for CSfC components located in the Red and Gray Networks. A Control Interface (CI) that is also a Cross Domain Solution (CDS) may be used to transfer the PSKs generated by the KGS from the Red Network to the Gray Network. The CIs that exist between the red management network and Red Network, and between the gray management and Gray Network, are not CDSs. They are CIs (e.g., firewalls) that control the flow of data between the management and data networks for both the red and gray portions of the CSfC solution.



**Figure 6: Connectivity Guidance for Locally Operated Key Generation Solutions**

Table 6 summarizes general requirement statements for KGS connectivity in CSfC solutions. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully and securely installing the KGS services into the CSfC solution network.

**Table 6: KGS Connectivity Requirements for CSfC Solutions**

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-38	PSK management services provided by a KGS (enterprise or locally operated) must be connected to the local red management network.	Installation of KGS services is to be performed in accordance with AO-approved installation instructions. Even if the KGS is not connected to the Red Network and operates in a	T=O



# Symmetric Key Management Requirements Annex



Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
		stand-alone configuration, the KGS is to be deployed in the Red Network enclave.	
PSK-39	If the KGS operates at the same classification level as the local red management network, a non-CDS CI must be used to control information flow between the KGS and the local red management network.	The information flows into and out of the KGS are to be well defined and only support the life-cycle management of PSKs. The CI (e.g., firewall) is to enforce these information flows and ensure no other information flows into and out of the KGS.	T=O
PSK-40	PSKs used for outer tunnel components operating on the Gray/Black network boundary must be distributed in accordance with an AO-approved method to move the PSKs from the Red Network to the Gray Network CSfC components.	No additional requirements.	T=O

## 2.3.6 KGS Audit Guidance

PSK management services are delivered by KGSs that operate in accordance with an approved KCMP. The KCMP defines the technical and procedural requirements for performing life-cycle management of PSKs. KGSs that deliver PSK management services for CSfC solutions are to comply with any audit and assessment requirements defined by the CSfC customer's operational security doctrine. The audits and assessments are to be performed by personnel who are knowledgeable in the KGSs' operations, as well as the KGSs' KCMP requirements and processes, respectively.

Table 7 summarizes general requirement statements for the auditing of a KGS. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in periodically auditing the KGS of the CSfC solution.

**Table 7: Additional KGS Audit Requirements for CSfC Solutions**

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-41	KGSs that deliver PSK management services for CSfC solutions must comply with audit and assessment requirements defined by the CSfC	AO-approved audit procedures are to be used to periodically audit and assess a locally operated KGS.	T=O



# Symmetric Key Management Requirements Annex



Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
	customer's operational security doctrine and enterprise KGS (if applicable).		
PSK-42	Audits and assessments must be performed by personnel who are knowledgeable in the KGS's operations, as well as the KGS's audit requirements and processes, respectively.	AO-approved audit personnel are to be used to periodically audit and assess a locally operated KGS.	T=O

## 2.3.7 PSK Testing Guidance

Life-cycle solution testing of PSKs should be performed prior to the operational deployment of KGS, using test PSKs vs. operational PSKs. The KGS should be capable of generating and distributing test PSKs to the DMs to validate the secure PSK distribution capabilities, as well as the installation of the PSKs onto the CSfC security devices. Use of the PSKs should be tested to ensure they can be used to mutually authenticate CSfC components and established the CSfC tunnels. Finally, the PSK update process needs to be tested (both for normal update functions and in response to a compromise scenario) to ensure the KGS is able to generate and distribute updated PSKs to DMs for installation onto the CSfC security devices.

Table 8 summarizes general requirement statements for the testing of a KGS. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully testing the KGS of a CSfC solution. Where applicable, CP requirements are identified to assist the CSfC solution owner in mapping the additional implementation requirements to specific KCM requirements defined in a CSfC CP.

**Table 8: PSK Testing Requirements for CSfC Solutions**

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-43	Life-cycle testing of PSKs must include initial generation and distribution of PSKs, installation and use of PSKs, scheduled updates of PSKs prior to PSK expiration, and PSK updates in response to PSK compromise.	AO-approved test plans and procedures are to be used to fully test the operations of a locally operated KGS.	T=O



# Symmetric Key Management Requirements Annex



## APPENDIX A. – ACRONYMS

Acronym	Meaning
AO	Authorizing Official
CDS	Cross Domain Solution
CI	Control Interface
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CP	Capability Package
CSfC	Commercial Solutions for Classified
CUI	Controlled Unclassified Information
DM	Device Manager
EUD	End User Device
IPsec	Internet Protocol Security
KCM	Key and Certificate Management
KCMP	Key and Certificate Management Plan
KGS	Key Generation Solution
MACsec	Media Access Control Security
MitM	Man-in-the-Middle
MSC	Multi-site Connectivity
NSA	National Security Agency
NSS	National Security System
NSSI	National Security Systems Instruction
PEK	PSK Encryption Key
PMO	Program Management Office
PSK	Pre-Shared Key
SRTP	Secure Real-Time Protocol
SSH	Secure Shell
TLS	Transport Layer Security
TPI	Two-Person Integrity
VPN	Virtual Private Network
WLAN	Wireless Local Area Network



# Symmetric Key Management Requirements Annex



## APPENDIX B. - REFERENCE

Document	Title	Date
CNSSI 4003	<i>Committee on National Security Systems (CNSS) Instruction Number 4003, Reporting and Evaluating COMSEC Incidents</i>	June 2016
CNSSI 4004	<i>CNSS Instruction (CNSSI) Number 4004, Destruction and Emergency Protection Procedures for COMSEC and Classified Material</i>	August 2006
CNSSI 4005	<i>CNSS Instruction (CNSSI) Number 4005, Safeguarding COMSEC Facilities and Materials</i>	August 2011
CNSSI 4009	<i>CNSS Instruction (CNSSI) Number 4009, Committee for National Security Systems (CNSS) Glossary.</i>	April 2015
CNSSP 7	<i>CNSS Policy (CNSSP) Number 7, National Policy on the Use of Commercial Solutions to Protect National Security Systems</i>	December 2015
CNSSP 11	<i>CNSS Policy (CNSSP) Number 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products</i>	June 2013
CNSSP 15	<i>CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the use of Public Standards for the Secure Sharing of Information Among National Security Systems</i>	October 2016
CSfC Campus WLAN CP	<i>Commercial Solutions for Classified (CSfC): Campus Wireless Local Area Network (WLAN) Capability Package (CP), v2.2</i>	June 2018
CSfC MA CP	<i>Commercial Solutions for Classified (CSfC): Mobile Access Capability Package (CP), v2.1</i>	June 2018
CSfC MSC CP	<i>Commercial Solutions for Classified (CSfC): Multi-Site Connectivity (MSC) Capability Package (CP), v1.1</i>	June 2018
CSfC KM Annex	<i>Commercial Solutions for Classified (CSfC): Key Management Requirements Annex, v2.0</i>	September 2020
IEEE 802.1AE-2018	<i>IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security</i>	December 2018
IEEE 802.1X-2020	<i>IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control</i>	January 2020
RFC 7296	<i>IETF RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2). C. Kaufman, et. al.</i>	October 2014
RFC 8784	<i>IETF RFC 8784 Mixing Preshared Keys in IKEv2 for Post-Quantum Security. S. Fluhrer, et. al.</i>	June 2020



# Symmetric Key Management Requirements Annex



Document	Title	Date
SP 800-57-1	<i>NIST Special Publication 800-57 Part 1 Rev. 5, Recommendation for Key Management - General.</i> E. Barker.	May 2020
SP 800-57-2	<i>NIST Special Publication 800-57 Part 2 Rev. 1, Recommendation for Key Management – Best Practices for Key Management Organizations.</i> E. Barker, et. al.	May 2019
SP 800-57-3	<i>NIST Special Publication 800-57 Part 3 Rev. 1, Recommendation for Key Management – Application-Specific Key Management Guidance.</i> E. Barker, et. al.	Jan 2015
SP 800-77	<i>NIST Special Publication 800-77 Rev. 1, Guide to IPsec VPNs.</i> E. Barker, et. al.	June 2020
	<i>CSfC Key and Certificate Management Guidance: Use Cases Appendix, Version 0.2</i>	June 2015
	<i>CSfC Key and Certificate Management Guidance, Version 0.7</i>	October 2015



# Symmetric Key Management Requirements Annex



## APPENDIX C. – SAMPLE STRUCTURE FOR A KEY AND CERTIFICATE MANAGEMENT PLAN (KCMP)

The following sample structure may be used to develop a KCMP for a locally operated KGS. The KCMP is required for CSfC solutions that use a symmetric Key Generation Solution (KGS) to generate and manage Pre-shared Keys (PSKs).

**TITLE:** Key and Certificate Management Plan for Pre-Shared Keys used in Support of <CSfC Customer Solution>

### SECTION 1: Introduction

This section identifies:

- The document as a KCMP for managing PSKs for the customer's CSfC solution.
- The type of CSfC solution (e.g., Mobile Access, Campus WLAN, Multi-site Connectivity), and which security tunnel(s) will use PSKs.
- The rationale for using PSKs in the CSfC solution.

### SECTION 2: CSfC Solution Overview

This section:

- Provides an overview of the CSfC solution, to include a diagram of the solution architecture that depicts the KGS in relation to the other CSfC components.
- Identifies whether an enterprise or locally operated KGS is used.
- Identifies the types and sizes of PSKs that will be generated by the KGS and used within the CSfC solution (this will typically be 256 bits for use with the AES algorithm).
- Provides a general overview of the key management concept for PSKs and the entities involved (both solution components and humans).

### SECTION 3: Key Management Plan

This section addresses the specifics of the key management plan for PSKs<sup>13</sup>. Diagrams showing information flows for PSK management functions are strongly encouraged throughout each section of the KCMP.

---

<sup>13</sup> If PSK Encryption Keys (PEKs) are used to protect PSKs during the life-cycle of the PSKs, PEKs are to be addressed as well in the KCMP. The sections in the KCMP apply to PSKs and PEKs.



# Symmetric Key Management Requirements Annex



## 3.1 Roles and Responsibilities

This section identifies all roles and responsibilities for performing the PSK management functions identified in the ensuing sections. Roles include the KGS Operator; KGS Administrator; KGS Security Officer; CSfC Device Manager; End User; and any other trusted roles to satisfy the PSK management requirements.

**KGS Operator** – Responsible for the general operations of the KGS to generate, distribute, manage and account for PSKs.

**KGS Administrator** – Responsible for the system administration of the KGS by ensuring its hardware and software baseline is maintained, and that the KGS is correctly configured to support the required operations.

**KGS Security Officer** – Responsible for ensuring the KGS is securely configured, and for periodically reviewing the audit logs for security critical events and other anomalies.

**CSfC Device Manager** – Responsible for managing the CSfC device that will use PSKs; securely installing PSKs into the CSfC device using TPI procedures defined in this KCMP; accounting for the PSKs installed on the CSfC device; destroying expired and compromised PSKs; and supporting PSK compromise recovery procedures.

**Other Trusted Roles** – Responsible for assisting KGS operations personnel and CSfC device managers with the secure life-cycle management of PSKs to ensure that no one person at any given time has sole access to plaintext PSKs used in the CSfC solution.

## 3.2 Key Request and Generation

This section identifies the procedures that will be used to request and generate PSKs for CSfC solution components. Specifically, this section addresses:

- Who is authorized to initiate a PSK request and for which CSfC solution component? If multiple CSfC solution components require PSKs, are different requesters used?
- What size PSK is requested and for which algorithm? Typically, the PSK will be 256 bits in support of AES.
- How does the PSK request identify multiple authorized recipients for the PSK? A PSK may need to be distributed to two different locations (e.g., VPN sites) that require the same PSK to establish a CSfC security tunnel.
- How is the PSK request sent from the requester to the KGS Operator (e.g., electronically, physically)? What is the format for the PSK request? Is it cryptographically protected (e.g., signed, encrypted)?



# Symmetric Key Management Requirements Annex



- How does the KGS Operator verify that the PSK request is authentic and from an authorized requestor? How does the KGS Operator verify that the recipients identified in the PSK request are authorized to receive the PSK?
- How does the KGS generate the PSK using TPI procedures? What is the media (electronic, physical) and specification format for the output containing the PSK?

## 3.3 Key Distribution and Installation

This section identifies the procedures that will be used to distribute and install PSKs onto CSfC solution components. Specifically, this section addresses:

- How is the PSK output from the KGS secured for distribution to the authorized recipients (e.g., CSfC Device Managers)?
- If the PSK output is encrypted:
  - How is it encrypted? Using a password-based encryption algorithm? Using a pre-placed PSK encryption key (PEK)? Using a quantum-resistant key distribution protocol?
  - How are TPI procedures applied to ensure that no one person can decrypt the PSK and recover it in plaintext form?
- If the PSK output is physical and in plaintext:
  - How is it packaged for secure physical distribution to the authorized recipients?
  - How are TPI procedures applied to ensure that no one person can gain access to the plaintext physical PSK?
- How does the authorized recipient of the PSK verify that the package containing the PSK (electronic or physical) has not been tampered with during distribution from the KGS to the Device Manager?
- How are TPI procedures applied to recover the plaintext PSK (e.g., decrypt, unwrap physical package) for installation into the CSfC solution component?
- How are TPI procedures applied to install the PSK into the CSfC solution component?
- How are TPI procedures applied to destroy all remaining copies of the PSK after it has been installed into the CSfC solution component?
- How are TPI procedures applied to ensure no one person can view or export the PSK in plaintext form after it has been installed on the CSfC solution component?

## 3.4 Key Update

This section identifies the procedures that will be used to update PSKs for CSfC solution components. Specifically, this section addresses:

- What are the circumstances that require the PSK to be updated (e.g., PSK expiration and regular update, compromise recovery, forced update for some other reason)?



# Symmetric Key Management Requirements Annex



- Under normal operations, how often are PSKs and PEKs updated?
- Is the PSK update process the same as the PSK request and generation process identified in Section 3.2 and 3.3? If not, explain any differences.

## 3.5 Key Compromise Reporting and Recovery

This section identifies the procedures that will be used to report the potential compromise of PSKs and to recover from PSKs deemed to be compromised<sup>14</sup>. Specifically, this section addresses:

- What are the incidents that may result in the compromise of a PSK? CNSSI 4003, Section VIII, identifies reportable COMSEC incidents, some of which are identified below as being mostly applicable to CSfC solutions<sup>15</sup>:
  - Cryptographic incidents – Any product malfunction or human error that adversely affects the security of PSK material. Examples include:
    - Unauthorized exposure of the PSK in plaintext form.
    - Use of expired PSKs.
    - Use of PSKs not generated by an NSA-approved KGS.
    - Use of defective PSKs that result in the transmission of classified information in plaintext form.
  - Personnel incidents – Any capture, attempted recruitment, known or suspected control by a hostile intelligence entity; intentional or unintentional exposure of PSK material to an unauthorized person; or unauthorized absence or defection of an individual having knowledge of or access to PSK material. Examples include:
    - Unauthorized disclosure of PSK material (to include unauthorized disclosure of PINs and passwords that are used to protect PSK material).
    - Attempts by unauthorized persons to affect such disclosure.
    - Deliberate falsification of PSK management records (e.g., accounting records).
  - Physical incidents – Any loss of control, theft, capture, recovery by salvage, tampering, emergency destruction, unauthorized modification, unauthorized viewing or access, or unauthorized photographing that has the potential to jeopardize PSK material. Examples include:
    - Unauthorized access to PSK material, including access by persons who are mistakenly believed to have held appropriate clearances.

<sup>14</sup> Information in this section is taken directly from CNSSI 4003. The term “COMSEC material” in CNSSI 4003 has been replaced with “PSK”. In some cases, the language from CNSSI 4003 has been modified to be more applicable to PSKs used in CSfC solutions.

<sup>15</sup> The reportable incidents identified in CNSSI 4003, Section VIII should be reviewed in their entirety to determine those incidents that are applicable to the CSfC solution.



# Symmetric Key Management Requirements Annex



- PSK material discovered outside of required PSK accountability or physical control.
  - Unexplained/undiagnosed zeroization or damage of PSK material.
  - PSK material improperly packaged.
  - PSK material improperly shipped.
  - PSK material received with a damaged inner wrapper.
  - Destruction of PSK material by other than authorized means.
  - Emergency destruction of PSK material.
  - Inadvertent or unintentional destruction or zeroization of PSK material, or destruction without authorization.
  - Evidence that product software configuration has been modified by non-authorized source or any un-authorized modification or update has taken place.
  - PSK material discovered to not have been destroyed within required time limits.
  - PSK material not completely destroyed as directed.
  - Actual or attempted unauthorized maintenance (including maintenance by unqualified personnel) or the use of a maintenance procedure that deviates from established standards. *[Note: This is applicable to the KGS and to the CSfC devices that use the PSKs.]*
  - Tampering with or penetration of PSK material.
  - Unexplained or unauthorized removal of PSK material from its protective technology.
  - Unauthorized copying, reproduction, or photographing of PSK material.
  - Loss of TPI or No-Lone Zone for PSK material.
  - Failure to perform audit trail management which results in subsequent loss of PSK material or data protected by the PSK material.
- What are the procedures for reporting a potential PSK compromise?
    - Who is authorized to report a potential PSK compromise?
    - To whom is the PSK compromise report sent? How is the compromise report sent (electronically or physically)?
    - How does the recipient of the PSK compromise report validate its authenticity and that the sender was authorized to submit the report?
    - Who is authorized to make the decision that a PSK is deemed compromised?
    - How is a compromised PSK reported to the parties that manage the CSfC solution components using the compromised PSK?
  - What are the procedures for updating the PSK due to a PSK compromise? Explain any differences from those procedures already identified in sections 3.2 through 3.4.

## 3.6 Key Backup and Recovery



# Symmetric Key Management Requirements Annex



This section identifies the procedures that will be used to perform backup and recovery of PSKs used in CSfC solutions. Specifically, this section addresses:

- Who is authorized to create backups of PSKs, and for what authorized purposes are the PSK backups required?
- What is the process to request the recovery of a backed up PSK, and how is that request validated to ensure the requester has an authorized need for the backed up PSK?
- Who is authorized to recover a backed up PSK and install it in a CSfC solution component?
- How do the recovery procedures ensure that the integrity of the PSK was maintained since it was originally backed up?
- How are TPI procedures applied to the PSK backup and recovery procedures to ensure no one person has access to the plaintext PSK?

## 3.7 Key Destruction

This section identifies the procedures that will be used to destroy PSKs (electronically or physically) such that they cannot be used in CSfC solutions. Specifically, this section addresses:

- What are the incidents that results in the destruction of a PSK? Examples include those incidents identified in section 3.5.
- Who is authorized to request the destruction of a PSK, and how is that request validated to ensure the requester is authorized to make such a request?
- Who is authorized to destroy the PSK?
- What means are used to destroy the PSK (electronic and/or physical)?
- What procedures are used to ensure all copies of a PSK are destroyed, especially of those copies exist in different physical locations?

## 3.8 Key Accounting

This section identifies the procedures that will be used to account for PSKs throughout their entire life-cycle. Specifically, this section addresses:

- How does the KGS Operator account for a PSK generated by the KGS? What identifier is used to uniquely identify the PSK (e.g., hash of PSK, manual recording of identifier)?
- How does the KGS Operator account for distribution of PSKs to CSfC Device Managers and other trusted entities, to include acknowledgment of receipt of the PSKs?
- How does a CSfC Device Manager or other trusted entity account for PSKs that are installed in CSfC solution components to support life-cycle management operations such as PSK update and compromise reporting?
- How do the accounting procedures ensure that a compromised or expired PSK is never used?



# Symmetric Key Management Requirements Annex



- How do the accounting procedures ensure that a rogue copy of a destroyed PSK is never used?
- How do the accounting procedures ensure that each PSK within a CSfC solution is identified uniquely?

## SECTION 4: References

This section lists any direct references made in the KCMP, as well as other informative references that assist in understanding the contents of the KCMP.